Antivirové programy

Možnosti ochrany

Ochranu před viry lze shrnout do **čtyř hlavních pravidel:**

1. **Zálohovat.** Je třeba zálohovat nutná data. Při dnešních cenách zálohovacích zařízení a při kapacitě jejich médií to není až tak velký problém.
2. **Používat výhradně legální programy.** Je však důsledně třeba dbát na to, aby toto pravidlo bylo skutečně striktně dodržováno, neboť často stačí jedna jediná hra, kterou někdo nelegálně instaloval na síti. U firem se používání nelegálního a hlavně zavirovaného programového vybavení na síti považuje za hrubé porušení pracovní kázně. Objevují se dokonce firmy, které ve snaze vyloučit užívání rizikového software nakupují pro své zaměstnance i počítačové hry.
3. **Nespouštět programy (a neprohlížet soubory) v příloze elektronické pošty od nedůvěryhodného zdroje.**
4. **Systematicky a pravidelně testovat počítače na přítomnost virů.** Žádný antivirový program sice nezaručuje absolutní bezpečnost, ale i snížení rozsahu škod o 70 %, které je při pravidelném používání běžných skenovacích programů reálné, znamená výrazné snížení finančních i jiných ztrát.

Obecné principy antivirových programů

Antivirové programy se podle principu vyhledávacích programů dělí obvykle do těchto skupin:

- **Skenovací programy.** Virus vyhledávají podle charakteristického řetězce, který je v jeho těle obsažen. Pro řadu virů lze takový řetězec nalézt. Často je to však složitější. Tímto způsobem např. nelze nalézt některé polymorfní viry. Řetězec musí být dostatečně dlouhý, aby antivir nevyvolával plané poplachy. S délkou řetězců a s jejich počtem pro různé viry však klesá rychlost kontroly. Tyto programy umožňují relativně jednoduchou antivirovou ochranu a narozdíl od rezidentních hlídačů nejsou příčinou různých technických a programových kolizí. Uživatel musí mít samozřejmě aktuální antivirovou databázi. Skenovací program pochopitelně nalezne jen známé viry, které jsou v jeho databázi
- Programy tohoto typu mohou též existovat jako rezidentní. Zvláštní skupinou jsou **heuristické skenovací programy,** které hledají v programech podezřelé instrukce, které obvykle viry užívají. Vyvolávají však plané poplachy a konečné rozhodnutí o tom, zda je soubor opravdu napaden, ponechávají na uživateli. Zde rozhoduje jen zkušenost uživatele, protože typické instrukce virů jsou zcela běžné u různých ovládačů a utilit.
- **Heuristická analýza** není rezidentní. Heuristický program emuluje počítač a provádí instrukce programu ve „virtuálním počítači“. Snaží se rozpoznat, zda program se chová „normálně“ – tedy pracuje jako běžný aplikační program či zda zde usiluje o neobvyklé akce typické pro viry. Tímto způsobem je možno odhalit viry dosud neznámé.

- **Hlídače kontrolních součtů.** Programy založené na tomto principu vytvářejí kontrolní součty souborů a zapisují kontrolní záznamy obsahující kontrolní součty, délku a atributy souborů. Následně pak kontrolují, zda v souborech nedošlo k nechtěným změnám. Tato metoda je velice spolehlivá a je účinná i proti dosud neznámým virům. Tyto antiviry mohou pracovat jako rezidentní a kontrolovat vybrané programy při každém spuštění. Nevýhodou je, že soubor s příslušnými daty musí být vytvořen ve stavu, kdy počítač není napaden virem. Navíc uživatel není upozorněn na konkrétní druh nákazy, pouze na podezřelé změny v souborech. Konečné rozhodnutí je opět na uživateli, neboť řada změn v souborech může být zcela legální, protože např. některé programy si zapisují údaje o konfiguraci samy do sebe.
- **Rezidentní hlídače neobvyklých činností (rezidentní štíty – on access scanners).** Jsou to rezidentní programy, které umožňují odhalit virus v okamžiku, kdy se pokouší provést rozmnožovací nebo destruktivní akci a této nežádoucí činnosti zabránit. Hlídají důležitá přerušení, sledují pokusy o formátování stop na discích a o změny v hlídaných souborech, zaměřují se rovněž na pokusy o instalaci nových rezidentních programů do paměti na změny v obsahu paměti CMOS. Tyto programy jsou často účinné i proti neznámým virům a navíc mohou zabránit i nechtěným smazáním souborů a formátováním disků samotným uživatelem. Avšak ani tato ochrana není dokonalá, neboť speciální viry jsou schopny obcházet různé rezidentní hlídače. I zde je důležitá zkušenost uživatele, protože existují (naštěstí nepříliš časté) programy a utility, které provádějí legální akce obcházením služeb operačního systému nebo provádějí akce podobné virům (např. zápisy do spustitelných souborů) a citlivý hlídač všechny tyto akce odhaluje. Rezidentní štít musí být dostatečně rychlý, aby významně nezpomaloval počítač.

Některé antivirové programy

- **F-Secure AntiVirus** je nová generace známého programu F-Prot. Obsahuje komplexní antivirovou ochranu pro všechny verze operačního systému Windows od 9x. Je k dispozici i v české verzi.
- **Kaspersky Anti-Virus Personal** v reálném čase vyhledává viry v adresářích i v příchozí a odchozí poště a brání jim ve vstupu do systému. Podporuje většinu běžných e-mailových klientů. Umožňuje odhalovat i dosud neznámé viry a umí odhalit i viry v komprimovaných souborech a opravovat archivy. Obsahuje i „záchranný balíček“ pro zprovoznění systému u všech běžných souborových systémů. Obsahuje i skener na požádání.
- **VirusScan** je světově uznávaný produkt se špičkovými detekčními schopnosti pro osobní počítače. Jeho antivirové řešení je:
  - **chytré –** skenuje na požádání nebo plánovaně,
  - **komplexní –** představuje řešení celistvé vhodné jako pro uživatelské stanice tak i pro souborové servery,
  - **malé –** instalační soubor je pouze 10 MB, velikost aktualizačních souborů je pouze okolo 100 KB,
  - **rychlé –** celkový výkon je optimalizovaný, aby nezdržoval uživatele,
  - **mobilní –** program je optimalizovaný i pro použití na mobilních zařízeních,
  - **přesné –** program je snadno spravovatelný lokálně i přes centrální správu.
- **Norman Virus Control** komplexní produkt na antivirovou ochranu síťových stanic i celých sítí. Je k dispozici i v české verzi
- **NOD 32** je slovenský produkt vyznačující se především účinnou heuristickou analýzou.

Zásady výběru antivirového programu

- **Přesně stanovit, co je třeba chránit** (disky, diskety, CD, internet a elektronická pošta) a podle toho volit antivirový program (např. zda má účinnou ochranu e-mailů).
- **Nekupovat krabicový produkt, ale komplexní řešení** tj. včetně možnosti dostupné technické podpory a pravidelných aktualizací.
- **Dbát na pravidelné aktualizace**
- **Antivirový program musí uživateli pomáhat a ne jej obtěžovat**
- **Viry je třeba hledat všude -** (dobrý program umí pracovat s archivy a umožnit skenovat libovolné přípony, případně rozpoznávat nutnost skenovat soubor nikoli podle přípony, ale podle hlavičky.)
- **Stoprocentní ochrana neexistuje,** nelze žádnému produktu bez výhrady důvěřovat.

Charakteristika antivirového systému AVG 7.0

Technologie

Testovací jádro je základem AVG, které si lze představit jako určitou „černou skřínku“, do které vstupují požadavky jednotlivých objektů a která vrací informace, zda jsou v pořádku, či zda byly infikovány. Testovací jádro je vybaveno rozhraním pro komunikaci s jednotlivými komponenty (rezidentní štít, moduly kontroly elektronické pošty), kterým poskytuje služby. Bylo vytvořeno s důrazem na maximální modulárnost celého systému AVG a je společné pro všechny komponenty.

Úspěšnost v odhalování virů je dáno kombinací několika úrovní detekcí. Nejprve se provede předzpracování testovaného souboru, včetně vyřazení částí nepodstatných z hlediska virové analýzy. Tím se dosáhne rychlého průběhu vlastního testování. Testování zahrnuje tyto detekční metody:

- **Detekce známých virů** – je nejjednodušší technikou a spočívá v odhalení známého viru pomocí sekvence, která je zanesená do virové databáze jako jeho identifikátor. Na základě tohoto typu nálezu se rozbíhá detailní analýza, vedoucí k jednoznačné identifikaci nákazy.
- **Generická detekce** je obecnější metodou detekce známých virů, užívanou pro rozpoznání jejich nových variant. Pokud není nalezen známý virus, hledají se sekvence typické pro určitý virus, které se obvykle nemění a nemusejí ani souviset s „virovým“ chováním. Tato metoda je účinná především při detekci makrovirů a skriptvirů.
- **Heuristická analýza** je poslední metoda hledání v případě neúspěchu detekcí. Jejím smyslem je najít virus, který dosud není ve virové databázi. V průběhu heuristické analýzy se používají dvě metody:
  - **Statická** heuristická analýza – hledání podezřelých datových konstrukcí,
  - **Dynamická** heuristická analýza – emulace kódu, to znamená jeho spuštění v chráněném prostředí virtuálního počítače uvnitř antivirového programu a hledání typických akcí, odpovídajících chování viru. Příkladem může být program, který vyhledává spustitelné soubory a modifikuje je.
- **Test integrity** je zjišťování informací o změnách spustitelných souborů na pevném disku což přispívá k odhalení nežádoucích změn a napomáhá léčit napadené soubory.

Detekční úrovně:

- **AVG pro email,** které je zajištěno buď ve formě doplňků pro příslušný emailový program nebo pomocí obecného emailového Scanneru AVG EMS, který pracuje na úrovni POP3 a SMTP protokolů a je tak nezávislý na konkrétním emailovém programu. Pomocí AVG EMS lze provádět filtraci souborů dle nežádoucích přípon či dle jejich obsahu.
- **Testy – kontrola na vyžádání (ON-DEMAND)** probíhají třemi způsoby:
  - **Plánované testy,** výrobce nastavil denní spouštění Kompletního testu. Uživatel si může plán testů upravit podle své potřeby, vytvořit si libovolné testy, určit, co kdy a co se má testovat a je zachovat v případě nálezu.
  - **Ručně spouštěné testy** lze spouštět kdykoli z uživatelského rozhraní. Typické užití je pro test výměnných médií.
  - **Nabídkou v Průzkumníku v rámci integrace AVG ve Windows.** Stiskem pravého tlačítka myši nad daným souborem lze vybrat nabídku „Otestovat systémem AVG“.
- **Rezidentní štít – kontrola při přístupu (ON-ACCESS),** který chrání počítač po celou dobu chodu operačního systému. Pracuje na pozadí, není závislý na ručním ovládání a ani na plánu. V případě nálezu nedovolí napadený soubor otevřít a spustit. Rezidentní štít AVG uchovává informace o kontrolovaných souborech a pokud nedošlo od okamžiku poslední kontroly k jejich modifikaci, nebo nebyla aktualizována virová databáze, nezdržuje uživatele opětovným prověřováním souboru.

Velmi důležitá je **aktualizace,** kterou lze provádět několika způsoby. Výrobce provádí aktualizaci 2 x týdně pravidelnými aktualizacemi a okamžitě dle potřeby mimořádnými aktualizacemi. Aktualizaci lze plánovat i provádět ji ručně podle tří úrovní jejich naléhavosti. Možnosti jak aktualizovat jsou:

- automaticky při připojení na internet (zejména při připojování se modemem)
- detekcí nového aktualizačního souboru v rámci plánovaných aktualizací
- ruční stažení aktualizace z internetu
- ruční aktualizace z adresáře nebo dodaného CD.

Literatura:

[1] Computerworld - ročníky 1995 a 1997
[2] Počítačové viry a Vy – součást manuálu programu AVG
[3] Bezpečnost dat – příloha Softwarových novin č 1/2001
[4] Přibyl, Tomáš a kol.: Počítačové viry v roce 200x, příloha PC WORLD – ročníky 2002, 2003 a 2004
[5] Antivirový systém AVG 7.0 , www stránky www.grisoft.cz